VOLUME 18 ISSUE 4

KCJIS NEWS

NOVEMBER 2016

NOTICE: CHANGE IN LABORATORY PROCEDURE
STEPHEN SISCO, LIMS ADMINISTRATOR KBI

Effective March 1st, 2017, laboratory reports will only be available online.

To ensure our customers receive the most efficient and effective services possible, the Kansas Bureau of Investigation (KBI) Forensic Science Laboratory activated the Laboratory Case Inquiry / Evidence Prelog segment of our Laboratory Information Management System (LIMS) in 2015. The Laboratory Case Inquiry feature serves a dual purpose. It allows our customers to view the current status of pending examinations and to easily download "released" laboratory reports. Through Laboratory Case Inquiry, laboratory reports are available immediately upon release to the customer, eliminating costly postal services and potential delivery delays.

In an effort to benefit from this technology and facilitate laboratory productivity, the KBI has decided to move away from providing hard copy reports to our customers. As of March 1st 2017, all laboratory reports will only be available and accessed online via Laboratory Case Inquiry. The KBI Forensic Science Laboratory will no longer mail laboratory reports to our customers except under extenuating circumstances.

Laboratory Case Inquiry is available to all KBI Forensic Science Laboratory customers through the Kansas Criminal Justice Information System (KCJIS) network. For detailed information on how to gain access to KCJIS (for new users) and Laboratory Case Inquiry visit the KBI's public website at http://www.kansas.gov/kbi/info/info_prelog.shtml. A Prelog Users Guide and instructional videos are also available on the website.

This information is being provided to all agency heads by email and/or mail. Please distribute this information to relevant staff members in your agency. If you have any questions please contact Steven D. Koch, Assistant Laboratory Director, at (785) 296-1117 or Stephen Sisco, LIMS Administrator at (785) 296-1130.

INSIDE THIS ISSUE

SUBMIT ELECTRONICALLY TO KIBRS
BROOKLYNN BRECKENRIDGE, PROGRAM CONSULTANT KBI

Is your agency interested in saving time, paper, stamps, and money? If so, now is the time to begin submitting electronically! Submitting electronically will eliminate your agency having to print and mail reports.

Listed below are the steps to begin submitting electronically:

1. Contact the Incident Based Reporting (IBR) Unit at (785) 296-4373.
2. Complete the application packet provided by the IBR Unit.
3. After the application packet is submitted and approved, the KBI Help Desk will install the KIBRS Gateway allowing you to electronically submit.
4. Work with a KIBRS Program Consultant to develop a plan for testing, a simple way to make sure everything is working smoothly.
5. We will work together to make sure any discrepancies are resolved and all requirements are being met.
6. Once approved, the agency will be notified with a date to start sending live reports electronically.

KSORT OFFENDER WATCH INTERFACE

JOHN GAUNTT, OFFENDER REGISTRATION UNIT MANAGER KBI
JENNIFER SLAGLE, PROGRAM CONSULTANT KBI

The Kansas Bureau of Investigation Offender Registration Unit (ORU) is dedicated to ensuring the public has access to accurate and timely information about the almost 18,000 registered sex, drug, and violent offenders in Kansas. This is done in conjunction with the local registering agencies (Kansas Sheriff's Offices and the Kansas Department of Corrections). The registry may be accessed at http://www.kbi.ks.gov/registeredoffender/ and is viewed approximately 1,600 times every day and for an average of four minutes per visit.

Approximately one year ago the ORU focused its energy on an Information Technology (IT) project with Watch Systems and its Offender Watch users in Kansas. The KBI IT department worked with Watch Systems to develop an interface that would allow Offender Watch users to submit their offender registration records electronically. After several months of dedicated work by many individuals on both sides, the interface started to accept electronic offender registration records in July 2016. Butler and Lyon County Sheriff's Offices were the first two Offender Watch users to submit electronic offender records through the interface.

To show how far we have progressed since July 2016, here are the numbers on two dates showing how offender records were submitted to the ORU in June 2016 and today. *Remember: all of the Offender Watch users were sending paper records that required data entry into the repository by ORU staff.*

Date	Offenders	KsORT users	KsORT records	Offender Watch users	Offender Watch records	Non-electronic users	Non-electronic user records
June 30	12,309	51	6,278	30	5,491	24	540
Nov 15	12,716	55	4,807	31	7,447	19	462

Notice that some county Sheriff's Offices made the switch to Offender Watch during this time; and some other Sheriff's Offices that formerly submitted paper records transitioned to KsORT.

Now let's see how the interface is progressing as of November 15th.

Offender Watch users submitting electronically	Offender Watch records submitted electronically	Offender Watch users submitting paper records	Offender Watch records submitted by paper
14	6,246	17	1,201

The remaining 17 Offender Watch users will progress into submitting electronic records through the interface upon completion of training and testing.

This recap shows that 11,053 of the 12,716 current offender registration records are now sent electronically to the KBI ORU. We are able to process the records more efficiently into the repository for our citizens. We hope that other counties will help us make further progress by choosing to use either KsORT or Offender Watch. If you have questions about KsORT, please contact Jennifer Slagle at (785) 296-0945 or Jennifer.Slagle@kbi.state.ks.us.

We are extremely grateful to all of the agencies and personnel involved with this interface project.

THE FBI'S NATIONAL DATA EXCHANGE (N-DEX)
KANSAS HIGHWAY PATROL CJIS UNIT

The Kansas Highway Patrol CJIS Unit received the following information from the FBI regarding N-DEx and wish to pass it along. It is a Kansas outreach document for users that wish to access N-DEx via RISS. For additional questions regarding N-DEx, please contact Stephanie Wisniewski. Her contact information is listed below.

The N-DEx System

* Go to the Law Enforcement Enterprise Portal (LEEP) at <www.fbi.cjis.gov> (Kansas Highway Patrol (KHP) users access the N-DEx System through a link on the KHP portal) * Click on N-DEx to conduct simple keyword searches or targeted searches for people, vehicles, locations, or property. * Eliminate information gaps through discovery of previously unknown relationships between people, events, property, and locations. * Use visualization tools to graphically depict associations, either on a link-analysis chart or on a map. * Set up subscriptions for ongoing investigations— receive automatic notifications of relevant information when new records enter the system, or when another user searches for the same criteria. * Use the batch query capability to upload and search multiple (up to thousands) people, vehicles, telephone numbers, etc., at one time. * Set up a collaboration space to work with criminal justice personnel across the nation, to instantly and securely share pertinent information, including files of any type or size.

Contact Information

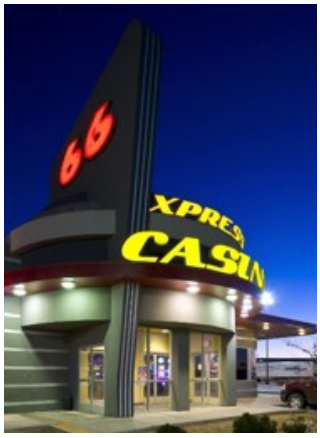
N-DEx Program Office: <ndex@leo.gov>
(304) 625-0555 <www.fbi.gov/ndex>
Kansas Liaison Specialist:
<Stephanie.wisniewski@ic.fbi.gov>
(304) 625-2146

What is N-DEx

The N-DEx System is a national investigative information-sharing system, enabling local, state, tribal, and federal criminal justice agencies to participate, at no cost. The N-DEx System is developed and managed by the Federal Bureau of Investigation's (FBI's) Criminal Justice Information Services (CJIS) Division. Records in the N-DEx System span the criminal justice lifecycle and include information related to incident/case reports, arrests, missing persons reports, service calls, booking and incarceration reports, pre-trial, probation and parole reports, warrants, citations/tickets, field contacts/field interviews, and most recently, photographs from Next Generation Identification. All of this information promotes public safety, from the initial patrol stop, to the supervision of an individual reintegrated into the community. The N-DEx System provides access to nearly 600 million records from more than 5,700 agencies, including over 2.5 million records from over 400 Kansas agencies. Federal data includes records from the Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms and Explosives, United States Marshals Service, FBI Field Offices, and the Department of Defense.

Value

The N-DEx System is a force multiplier for you, the officer or investigator who needs more information in less time, and can be used to exhaust every lead. The following FBI N-DEx 2016 Success Story of the Year demonstrates the benefits of using the N-DEx System:



N-DEx helps solve casino robbery

On December 13, 2015, the Route 66 Casino Express in Albuquerque, New Mexico, was robbed. Two male subjects entered the casino, pointed a loaded firearm at one of the cashiers, and demanded money. Meanwhile, a female accomplice stayed outside in their get-away vehicle. Minutes prior to the robbery, the unknown female accomplice swiped a casino rewards card to pay for fuel at one of the pumps nearby. The Pueblo of Laguna Police Department and the FBI were called to investigate. With limited information on the female subject, a special agent with the Laguna Police Department contacted the Rocky Mountain Information Network (RMIN). The agent spoke to a criminal intelligence analyst, asking her to find out what she could on the female driver. By searching the FBI's N-DEx System, multiple records were discovered that revealed the identities of the female and her criminal associates. The agent then took the information gathered from the N-DEx System to two RMIN Intelligence Research Analysts, for full background checks and criminal intelligence packages. With the volume of detailed information gathered by using the N-DEx System and other intelligence databases, three arrests and two confessions were obtained. The agent stated, "The true heroes in the case were the intelligence analysts that provide us with the information and the direction in which to proceed."

2017 KCJIS CONFERENCE—SAVE THE DATE!
GORDON LANSFORD, DIRECTOR KCJIS

The 2017 KCJIS Conference will be held June 4-6, 2017 at the Ramada Inn and Conference Center in Topeka. If you have any questions or suggestions regarding the conference, please contact Gordon Lansford at (785) 633-7700 or Gordon.Lansford@ks.gov.

KBI TRAINING OPPORTUNITIES IN 2017
JESSICA CROWDER, PROGRAM CONSULTANT KBI

The Kansas Bureau of Investigation (KBI) has now set their field support training schedule for 2017. This year, all training sessions will take place at KBI Headquarters in Topeka. To attend any of these complimentary training sessions, please register with the KBI receptionist at AnnexFrontDesk@kbi.state.ks.us or (785) 296-7404. If you are unable to attend training, please contact one of the individuals below to discuss alternatives.

Training Dates:

- March 1st and 2nd
- June 28th and 29th
- October 18th and 19th

Courses offered:

- 10 Print Fingerprint Identification
- Offender Registration
- KsORT
- Central Message Switch/ KCJIS Web Portal
- Criminal History Records
- Rapsheet Differences
- Kansas Incident Based Reporting System (KIBRS)

10 Print Fingerprint Identification
Tina Ortega
(785) 296-4483
Tina.Ortega@kbi.state.ks.us

Offender Registration/KsORT
Jennifer Slagle
(785) 296-0945
Jennifer.Slagle@kbi.state.ks.us

Central Message Switch/ KCJIS Web Portal
Javier Barajas
(785) 296-6832
Javier.Barajas@kbi.state.ks.us

Criminal History Records/Rapsheet
Vanessa Rine
(785) 296-0816
Vanessa.Rine@kbi.state.ks.us
OR
Jessica Crowder
(785) 296-8338
Jessica.Crowder@kbi.state.ks.us

KIBRS
Connie Molina
(785) 296-8278
Connie.Molina@kbi.state.ks.us
OR
Brooklynn Breckenridge
(785) 296-7945
Brooklynn.Breckenridge@kbi.state.ks.us

KCJIS SECURITY INCIDENT RESPONSE
KIP BALLINGER, IT SECURITY AUDITOR/TRAINER KHP CJIS UNIT

Are you and your Agency prepared for a security incident?

Do agency personnel know what to do in the event of a security incident?

Are there procedures / policies in place and have they been communicated and taught to organizational stakeholders?

The reasons for having a good written security incident response plan and procedures are many. Not only because having one is required by KCJIS Security Policy, but by making the preparation in terms of policy formation, communicating the procedures, and response training, the agency can more effectively detect, contain, and recover from a security incident.

A security incident can include breaches of physical security, lost or stolen laptops, hand-held devices (smart phones, tablets, etc.) or storage devices, lost or stolen paper files, which contain Criminal Justice Information (CJI), breaches of cyber / information systems, etc.

KCJIS SECURITY INCIDENT RESPONSE, CONTINUED

KIP BALLINGER, IT SECURITY AUDITOR/TRAINER KHP CJIS UNIT

KCJIS Security policy defines Computer Security Incident Response Capability (CSIRC) as a collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur. Additionally, the agency should have this not only for computer security incidents, but also for other types of security incidents, including breaches of physical security, lost or stolen devices, electronic media, or paperwork which contains CJI.

Policy section 5.3.2 (Management of Security Incidents) states that a consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

Policy section 5.3.2.1 (Incident Handling) requires that an agency implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The agency must employ automated mechanisms to support the incident handling process wherever feasible. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

An agency's Security Incident Response Plan should be viewed as a living document, whereby the policies and the incident response procedures are modified accordingly in real time as the lessons are learned from ongoing incident handling activities. Having a good response plan with procedures in writing is a good thing, but if agency personnel do not know the procedures to recognize and respond to an incident, it is of no value. This requires communication and training.

Do agency personnel know what do in the event of a security incident? If malware is suspected on a computer, is it best to shut the computer off or simply to unplug it from the network and call the I.T. personnel immediately? Policy section 5.3.3 (Incident Response Training) states that the agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

Level One Security Awareness Training (Policy section 5.2.1.1) lists the minimum topics that shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location. That list includes 'incident response' (Identify points of contact and individual actions) and 'visitor control and physical access to spaces' (discussion of applicable physical security policy and procedures, e.g., challenge strangers (stranger-danger), report unusual activity, etc.)

Once an incident is discovered, it must be reported. Policy section 5.3.1 (Reporting Security Events) requires this reporting, as well as having formal event reporting and escalation procedures in place. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

The individual at the local agency who discovers the security incident shall immediately notify their agency LASO or agency supervisory personnel and the KBI Help Desk. The agency shall take appropriate steps to identify, contain, isolate and document the incident as quickly as possible (Information Technology personnel may be enlisted to assist). (Policy section 5.3.2.1 - Incident Handling). Depending upon the nature of the security incident, access to KCJIS may be suspended until the incident is resolved.

Security incidents must be reported using the KCJIS139 form (Security Incident Notification), which can be found on the KHP Launchpad at https://cjisaudit.khp.ks.gov/launchpad/cjisdocs/files/kcjis139_security_incident_notification_112013_distributed.pdf. On this form, the agency documents in writing what steps have been taken to secure its site. KHP CJIS staff then reviews the document to determine whether or not the agency security requirements have been successfully addressed. If so, an authorization to resume KCJIS access is issued. If not, additional steps will be required by the agency before authorizing resumed KCJIS access.

A good practice for recovering from cyber security incidents is to have Backup and Disaster Recovery Plan in place as part of the agency's Security Incident Response Plan. This includes the practice of backing-up important files and having current images available for hard drive failure or instances of encrypted files due to ransomware. Below, are some helpful links to develop a Security Incident Response Plan:

http://cybersecurity.alabama.gov/documents/Policy_604_Incident_Response.pdf

http://www.cio.ca.gov/OIS/Government/library/documents/Incident_Response_Plan_Example.doc

Computer Security Incident Handling Guide Special Publication 800-61 Revision 2

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

https://www.cert.org/incident-management/products-services/creating-a-csirt.cfm

https://www.ready.gov/business/implementation/IT

KCJIS NEEDS YOU!
MELISSA WEISGERBER, IT PROGRAM CONSULTANT KBI

The Kansas Bureau of Investigation is looking forward to launching the KCJIS User Groups across the State. In the interest of maintaining broad participation, we need to develop main points of contact within each identified region to assist us as a liaison in organizing and scheduling meetings as needed by each region. The demands on your time are already significant, and it is important that each region develop a timetable and typical agenda that will fit your needs; your input into these groups is critical to their success. In turn, the success of these groups is critical to the continued growth and success of KCJIS.

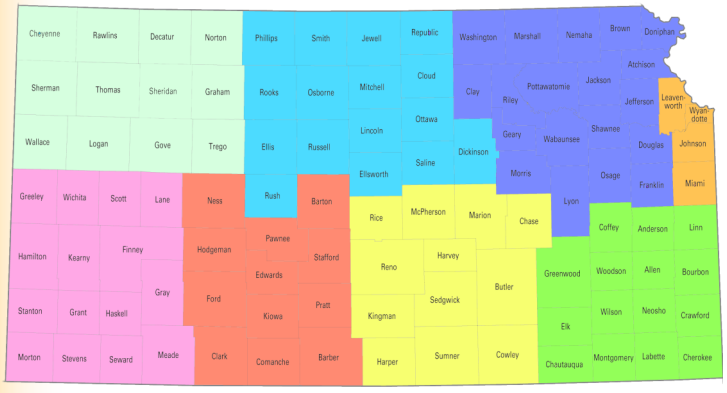
Some of the expected benefits of a strong network of KCJIS User groups across the state:

- Solid communication across the state on subjects that matter to you
- Shared experience and strength of community, particularly within each region
- The ability to provide direct input on new systems and changes being considered or implemented
- The ability to be a voice for what your region needs
- A way to communicate across different areas of practice within the criminal justice community
- Direct feedback and guidance to state agencies
- Exchange of operational information between agencies within your region

We will be numbering the regions, and emailing interested community members in each region to begin setting up and scheduling meetings. Initially, meetings will be held quarterly, but this can change based on whatever needs your region has. There are a few things that we ask of you to make this a success:

- Please send us topics for discussion that matter to your agency or region
- If you have ideas for a place to meet that works well for your region, please let us know
- If there are particular times that work best for your region, please let us know
- If you have an interest in becoming more involved, please ask

PROPOSED KCJIS USERS GROUPS REGIONS



DRAFT COPY

Meetings will be announced via email, on the KCJIS Portal, via the Central Message Switch (over OpenFox), and in this Newsletter.

Please contact Melissa Weisgerber for further questions, or to send in any topics, ideas, times, or to show your interest.

Melissa Weisgerber

Information Technology Program Consultant

Kansas Bureau of Investigation

Desk: (785) 296-8281

Cell: (785) 213-5187

Melissa.Weisgerber@kbi.state.ks.us

NEWS FROM THE KBI HELP DESK
JAVIER BARAJAS, NETWORK CONTROL TECHNICIAN III KBI

Kansas VINE Service

Victim Information Notification Everyday documents are posted on the KCJIS Web Portal Information tab under the KS State Systems section within the KS DoL Victim Information Notification System heading. This effort is supported by the Kansas Sheriffs' Association (KSA), the Office of the Attorney General, and the Kansas Department of Labor, (KDOL). Implementation of Kansas VINE continues through 2017. For regional training and other information please visit www.vinelink.com or download the free mobile app, VINEMobile. The Kansas VINE Toll-free number is 1-866-KS-4-VINE.

KCJIS Message Switch Platform

The KBI Help Desk and Computer Projects of Illinois have recently finished a platform change to the KCJIS Central Message Switch, (CMS). The new Linux based platform will provide a more robust and stable platform. The changes made on Sunday 11/13/16 were transparent to CMS users.

KCJIS Security Policy v5.4

KCJIS Security Policy v5.4 calls for increased authentication security. All 4 and 5 digit token PIN numbers are increased to 6-8 digits. The KBI Help Desk started enforcing this new policy on an agency by agency basis starting Monday Oct 31st 2016 and continues through the end of the calendar year. Once your agency's enforcement date arrives you then are required to change your PIN. Please contact your TAC for your agency's specific enforcement date. More information including new PIN criteria can be found on the KCJIS Web Portal. Visit https://kcjis.ks.gov and find the 'RSA Token PIN Change Instructions' under the Information tab, Security Polices section. The complete KCJIS Security Policy v5.4 is also available in the same location.

KCJIS User Group

At the November meeting the group continued a discussion on Kansas Open Records Act, KORA. A short update on the Kansas Misdemeanor File merger to NCIC was also provided by KBI IT Developers group. Our next meeting is January 5th at the KBI HQ. If you are interested in a meeting in your area of the State, contact Melissa Weisgerber at Melissa.Weisgerber@kbi.state.ks.us or 785-296-8281.

THE INTERNET OF THINGS THIS HOLIDAY SEASON
DON CATHEY, KCJIS INFORMATION SECURITY OFFICER KHP

As this holiday shopping season grows into the mad dash, many new technology gadgets are being advertised to try to capture everyone's gift giving dollars.

Before you rush to order that cool toy, video camera system, thermostat, Wi-Fi connected voice response unit, or any other myriad of new gizmos that you can manage or access on your smart phone, you may want to pause and consider some cautionary information about those trendy techy devices that are part of what has been named "the Internet of Things".

So you are asking: "What does my smart thermostat at home have to do with KCJIS?" Well, maybe nothing.

BUT, if your thermostat is being controlled by malcontents to disrupt access to other important networks and information systems (see the US-CERT Alert TA-288A8*), it may have a lot to do with KCJIS! Or, if your Internet of Things device is used to compromise your identity, your whole life can be adversely affected.

** The United States Computer Emergency Readiness Team (US-CERT) has prepared some articles that discuss the security risks of the Internet of Things. We have saved these articles - along with others that address other technology concerns - to the KHP CJIS Launch Pad > CJIS Documents > TECHNICAL SECURITY INFORMATION > Internet of Things.*

The KCJIS Newsletter is published in cooperation of the Kansas Criminal Justice Coordinating Council and KCJIS Committee

KCJCC Committee Members

Derek Schmidt
Attorney General
Chair

Sam Brownback
Governor
Vice-Chair

Kirk Thompson
Director
Kansas Bureau of Investigation

Justice Caleb Stegall
Chief Justice Designee

Joe Norwood
Secretary
Kansas Department of Corrections

Mark Bruce
Superintendent
Kansas Highway Patrol

KANSAS BUREAU OF INVESTIGATION

Jessica Crowder
Newsletter Editor
1620 SW Tyler
Topeka, KS 66612
(785) 296-8338
Jessica.Crowder@kbi.state.ks.us

KCJIS Committee Members

Capt. Justin Bramlett
Kansas Highway Patrol
Chair

Sec. Sarah Shipman
KS Department of Administration
Vice-Chair

Capt. Lance Royer
KS Sheriffs Association
Treasurer

Ed Klumpp
KS Association of Chiefs of Police
Immediate Past Chair

Leslie Moore
Kansas Bureau of Investigation

Harold Sass
KS Department of Corrections

Kelly O'Brien
Office of Judicial Administration

Pam Moses
KS Association of District Courts

Amber Norris
KS County and District Attorney Association

Bill Duggan
Lyon CO ECC
KS Assoc. of Public Communications Officers